Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Digital Broadcast Content Protection) **MB Docket No. 02-230**
)

PETITION FOR RECONSIDERATION AND CLARIFICATION OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

Jon A. Baumgarten
Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street NW, Suite 800
Washington, DC 20036
(202) 416-6800

Counsel for The Motion Picture Association of America, Inc.

January 2, 2004

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	
Digital Broadcast Content Protection	**)**	**MB Docket No. 02-230**
	)	

PETITION FOR RECONSIDERATION AND CLARIFICATION OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

INTRODUCTION AND SUMMARY

The Motion Picture Association of America, Inc. ("MPAA") welcomes the Commission's adoption of the Broadcast Flag regulation.[1] The Commission's action is a substantial and important step forward in achieving the protection of free over-the-air broadcast digital television, and the MPAA greatly appreciates all of the work the Commission has done over the past several months in bringing the Broadcast Flag regulation to fruition.

The Commission has stated that its goal in adopting the Broadcast Flag regulation is to "ensure the continued availability of high value DTV content to consumers through broadcast outlets." Broadcast Flag Order ¶ 8. In order to achieve this goal, broadcast DTV content must receive protection equivalent to that available in other distribution channels, or it will inevitably migrate to where it is better protected, with consequent harm to consumers. Content protection has two, critical components: (1) the security of outputs and recording methods, and (2) the robust construction of DTV devices themselves. Both elements are necessary for a complete content protection system. Even if the outputs and recording methods are truly secure, if DTV

[1] *See* Report and Order and Further Notice of Proposed Rulemaking, *Digital Broadcast Content Protection,* M.B. Docket No. 02-230, FCC 03-273 (rel. Nov. 4, 2003) ("Broadcast Flag Order").

devices themselves are constructed in a manner such that digital content can be readily accessed in the clear, the Broadcast Flag protection scheme will not achieve its objective.

The rules governing the robust construction of DTV devices are thus an equally important component of the Broadcast Flag regulation. For the reasons stated below, however, the Robustness Rule adopted by the Commission establishes a weaker robustness standard than commonly accepted and used in the marketplace for other protected distribution channels. Improvement of the regulation is therefore needed in order to ensure that the Commission's goal in adopting the regulation is achieved.

The robustness standard proposed by the MPAA and others can be implemented with no material increase in cost for manufacturers or consumers, and no loss of flexibility for manufacturers in designing their devices. Recognizing the value of the immediate implementation of the existing regulation, the MPAA proposes that the existing Robustness Rule remain in effect for an interim period after adoption of the robustness rules proposed herein, which would become effective eighteen months after public notice of their adoption.

As a clarification, the MPAA also requests that the Commission revise the text of its Order to make clearer that manufacturers of add-in computer products using "Robust Method" transfers must ensure that Marked and Unscreened Content are not available in unencrypted, compressed form via a User Accessible Bus.

I. The Commission Should Reconsider Its Robustness Rule to Account for the Viral Proliferation of Hacks From Compromised Devices

Contemporaneous with the Broadcast Protection Discussion Group ("BPDG") effort, the MPAA, the 5C companies,[2] and the Computer Industry Group ("CIG") – a predecessor of the IT

[2] The "5C companies" are the five member companies of the Digital Transmission Licensing Authority ("DTLA"), namely, Intel Corp., Hitachi Ltd., Matsushita Electric Industrial Co. Ltd., Sony Electronics Inc., and

Coalition – engaged in trilateral negotiations to develop rules for protecting broadcast DTV content. Those trilateral negotiations resulted in a joint proposal, based on previous marketplace content protection agreements, containing a set of robustness rules, compliance rules, and criteria for Authorized Digital Output Protection Technologies and Recording Methods (the "Joint Proposal").[3] The robustness rules contained in that Joint Proposal, set forth at Sections X.7 to the italicized note after X.11 (the "Jointly Proposed Robustness Rules"), are essentially the same provisions put forward by MPAA and the 5C companies in this proceeding.[4]

The Jointly Proposed Robustness Rules received unanimous agreement among MPAA, 5C, and CIG, and received widespread endorsement from the remainder of the BPDG participants as well. Indeed, Section 4.9 of the BPDG Report notes that "[g]eneral agreement has been reached as to the specific robustness requirements to be implemented by covered products." The only issue on which any substantial disagreement was expressed was whether to define the specific robustness requirements with reference to the skill level of a "user" rather than a "professional."[5] That is, some parties in the BPDG proposed inserting the phrase "by a user" in various places in the Jointly Proposed Robustness Rules; they did not propose eviscerating them.[6] Thus, while refinements to the Jointly Proposed Robustness Rules were

Toshiba Corp.

[3] *See* Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group ("BPDG Report"), June 3, 2002, Tab F-2.

[4] The IT Coalition has evidently withdrawn its support for the Joint Proposal, even though the members of CIG and the members of the IT Coalition are virtually identical.

[5] Note that the IT industry was not among the parties making this objection in the BPDG. *See* Joint Proposal §§ X.7 – X.11. In the IT Coalition's initial comments in this proceeding, the IT Coalition did not propose scrapping the Jointly Proposed Robustness Rules, but rather proposed inserting the term "user" in Sections X.7(a), X.9(b)(2), X.9(c)(2), and X.11(a). *Notably, the IT Coalition did not propose adding the term "user" to Section X.11(b), which requires DTV devices to implement the Compliance Rules such that they "[c]an only with difficulty be defeated or circumvented using professional tools or equipment . . . such as would be used primarily by persons of professional skill and training."*

[6] *Compare* Joint Proposal §§ X.7 – X.11 *with* BPDG Report, Tab C-1 ("BPDG Proposal") §§ X.7 – X.11. In

proposed in the BPDG,[7] no IT or CE manufacturer claimed that the Jointly Proposed Robustness Rules were unworkable; nor, given the widespread marketplace acceptance of those rules, would such an argument have even been plausible.

In its November 4th order, the Commission adopted much of the Joint Proposal, but declined to adopt the Jointly Proposed Robustness Rules. The Commission concluded that "an expert level of robustness exceeds that which is needed to effectively implement an ATSC flag regime" because all that is needed is to protect against security breaches by "ordinary users."[8] However, the Commission went much farther than resolving the limited debate over whether to insert the term "User." Instead, the Commission eliminated virtually the entirety of the carefully drawn set of Jointly Proposed Robustness Rules and replaced them with a single standard:

> The content protection requirements set forth in the Demodulator Compliance Requirements shall be implemented in a reasonable method so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment.

The Commission further defined "generally available tools or equipment" as "tools or equipment," including "specialized electronic tools or software tools," that are "widely available at a reasonable price."[9]

the BPDG Proposal, "user" was tentatively defined as any consumer who was not "a professional trained to build, repair or service a Covered Product." It should be noted that this proposed edit to the Jointly Proposed Robustness Rules would have been a departure from the many other content protection agreements in the marketplace today, none of which peg their robustness rules to the skill level of a "user" of the product.

[7] A few parties also objected to requiring devices to "effectively frustrate" attempts to defeat the Compliance Rules, even though that phrase has been employed without incident in numerous content protection agreements. *See* BPDG Report ¶ 5.5; BPDG Proposal at 10 n.31; *but see, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 1.1; HDCP License Agreement, Exh. D, ¶ 1.1; DFAST ¶ 1.1; PHILA ¶ 1.1; CPRM License ¶ 3; CSS Procedural Specifications ¶¶ 6.2.4.1, 6.2.5.1. Again, the IT industry was not among those in BPDG suggesting this change.

[8] Broadcast Flag Order ¶ 46.

[9] 47 C.F.R. § 76.9007.

A. **The Robustness Rule Adopted by the Commission Fails to Ensure That the Goal of the Broadcast Flag Regulation Will Be Achieved**

In explaining its conclusion that "an 'ordinary user' level [of robustness] is appropriate in these circumstances," the Commission cited, in part, the Joint Reply Comments of the MPAA, *et al.* ("Joint Reply Comments"), in which the MPAA and others stated that:

> A person who hacks their device will simply achieve the disabling of that single device, and no other impact. . . . The Broadcast Flag will keep widespread unauthorized redistribution under control because most consumers will not hack their devices.[10]

The Commission concluded from this that "an expert level of robustness is incongruous with the scope of protection offered by an ATSC flag system."[11] The Commission's conclusion merits reconsideration for two reasons. First, the section quoted from the Joint Reply Comments in support of the Commission's decision *presumed the adoption of the very rules the Commission declined to adopt*. In the world envisioned in the Joint Proposal, where devices are robust, hacks will likely result only in the "disabling" of the device pursuant to the requirements of Sections X.9(b)(2) and X.9(c)(2), which the Commission eliminated. Even if an attack manages to compromise the security of a device without disabling it or revoking its device authorization, such hacks would be extremely rare if the Joint Proposal were adopted, and would at most affect devices of a particular model made by a single manufacturer. The rule adopted by the Commission, however, eliminates Section X.9 as well as most of the other Robustness Rules, meaning that hacks of compliant devices are likely to be much more frequent and severe, are more likely to result in the device being able to continue operating notwithstanding the hack, and may overwhelm the ability of content owners to handle compromised devices through alternative means, such as legal remedies.

[10] Joint Reply Comments at 16.

Second, and of paramount importance, the passage quoted from the Joint Reply Comments, and the Commission in turn, telescoped three distinct goals: (1) the prevention of widespread unauthorized redistribution of digital broadcast content; (2) the prevention of compromises that will allow more than a *de minimis* leakage of content; and (3) the prevention of compromises that can themselves be widely circulated. The first goal is impossible to achieve without the latter two, but in order to achieve the latter two goals, it is not the "ordinary user" that needs to be thwarted, but the skilled user. Experience demonstrates that it is the skilled few that first develop a hack, and then widely distribute the fruits of that hack to others, whether it is content in the clear traded on peer-to-peer networks, or a software utility that executes the hack and makes it possible for non-experts to implement it. As the Director of IT Security for the GAO has noted with respect to computer security:

> Frequently, skilled hackers develop exploitation tools and post them on Internet hacking sites. These tools are then readily available for others to download, allowing even inexperienced programmers to create a computer virus or to literally point and click to launch an attack. According to a NIST publication, 30 to 40 new attack tools are posted to the Internet every month.[12]

The issues for computer security are similar to those for content security. For every skilled hacker who is able to break into a website, there are a hundred or more tyros whose only technical knowledge lies in running programs written by others that find website vulnerabilities. Similarly, for every person who writes a program such as DeCSS, there are thousands who can run that program on their computers or can download and redistribute hacked content from websites and peer-to-peer networks. It is true that DVDs are still a profitable distribution

[11] Broadcast Flag Order ¶ 46.

[12] *Computer Virus Protection: Hearing Before the House Subcomm. on Tech., Info. Policy, Intergovernmental Relations, & the Census, House Gov't Reform Comm.*, 108th Cong. (Sept. 10, 2003) (statement of Robert Dacey, Director, IT Security, General Accounting Office).

channel, even though their security has been compromised. However, the experience of the music industry demonstrates that there is a time interval between when the problem of unauthorized redistribution over networks such as the Internet first manifests itself and when it begins to have a serious financial impact. As the Commission has noted, "the threat of widespread indiscriminate retransmission of high value digital broadcast content . . . is forthcoming and preemptive action is needed . . . ."[13]

The IT Coalition's suggestion that the appropriate level of robustness "assumes ordinary users as attackers rather than experts"[14] thus blithely ignores common experience, including that of the computer industry itself. The members of the IT Coalition clearly do not secure their own interests under the same standard.[15] At its core, their assertion is based on the notion that broadcast DTV content is somehow of lesser status than other properties, including other forms of television distribution. This is both unprincipled and wholly at odds with the Commission's stated purpose in this proceeding to foster the DTV transition and ensure the continued viability of DTV broadcasting.

There is thus good reason for the nearly unanimous requirement in marketplace robustness rules that a robust product be capable of frustrating attempts to defeat the Compliance Rules made not just by an "ordinary user," but also by experienced users. Even though most consumers will not hack their devices, a significant number of ordinary consumers may download, install, and redistribute the products of hacks by others. A level of robustness

[13] Broadcast Flag Order ¶ 4.

[14] *See* Broadcast Flag Order ¶ 45.

[15] Software manufacturers regularly rebuff exploits as those using the Remote Procedure Call vulnerabilities in the Windows operating system that Microsoft discovered and patched earlier this year. *See* Matthew B. Stannard, *Strange Tale of How Clumsy Blaster Worm Dug Its Hole,* S.F. Chron., Aug. 16, 2003, at A10. If IT companies designed to an "ordinary user" standard, their products would repel barely any attacks at all.

that deters only "ordinary users" will therefore not provide much of a roadblock for unauthorized redistribution. In fact, the Commission itself has recognized in other contexts that the level of robustness necessary to successfully protect content must prevent hacks that even only a skilled few can carry out.[16] The Broadcast Flag Robustness Rules, to be most effective, must lower the probability of a successful hack to the point where it becomes feasible, legally and logistically, to deal with those rare compromises that do occur.

The lesser level of robustness required in the Broadcast Flag regulation impacts the security of outputs as well. As discussed more fully below,[17] in two cases, the Broadcast Flag permits self-certified digital "Robust Method" transfers to be made instead of transferring over Authorized Digital Output Protection Technologies. Formerly, the level of robustness for such transfers was specified in Section X.10 of the Joint Proposal, which required, for example, for transfers from an add-in computer product, that the Robust Method be "reasonably secure from being intercepted, redistributed or copied when being so passed to such other product." This level of robustness was critical to the compromise that allowed Robust Method transfers to exist in the Joint Proposal in the first place. Now, however, Robust Methods are defined with reference to Section 73.9007, and therefore must only be "implemented in a reasonable method

[16] The Commission wisely chose, in adopting a requirement that "scanning receivers" be "incapable of . . . readily being altered by the user to operate . . . within the frequency bands allocated to the Cellular Radiotelephone Service," to define "capable of readily being altered" in terms of what skilled user rather than an ordinary user would know how to do. *See* 47 C.F.R. § 15.121(a)(1) (prohibiting modification of scanning receivers by, e.g., "replacing a plug-in semiconductor chip; or programming a semiconductor chip using special access codes or an external device, such as a computer"). In a provision reminiscent of Section X.9(c)(2) of the Joint Proposal, the rule also provides that scanning receivers be designed "such that any attempts to modify the equipment to receive transmissions from the Cellular Radiotelephone Service likely will render the receiver inoperable." *Id.* § 15.121(a)(2). In adopting this rule, the Commission noted that the Consumer Electronics Manufacturing Association "indicates that it sees no other reasonable alternative available to help guard the privacy of cellular telephone conversation[s]." Report and Order, *In the Matter of Amendment of Parts 2 and 15 of the Commissions Rules to Further Ensure That Scanning Receivers Do Not Receive Cellular Radio Signals*, E.T. Docket No. 98-76, FCC 99-58, ¶ 18 (rel. Mar. 31, 1999).

[17] *See* page 16.

so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment." As a result, not only are DTV devices less secure under the Commission's Robustness Rule than they should be, but so are many outputs.

The Commission should therefore reconsider its decision and adopt the carefully negotiated and marketplace-derived Jointly Proposed Robustness Rules attached to this Petition. As explained further below, those rules have been demonstrated by the marketplace and by experience to represent the appropriate level for the protection of copyrighted content. Contrary to what has been argued by some, the Jointly Proposed Robustness Rules will not place a significant burden on manufacturers or consumers. If the rules as proposed by MPAA, 5C, and others are not adopted, it will be significantly more difficult to achieve the goal of the Broadcast Flag regulation.

B. The Carefully Drawn Set of Jointly Proposed Robustness Rules Are the Industry Standard for the Protection of Copyrighted Content and Rely Upon the Real-World Experiences of Multiple Industries

The Jointly Proposed Robustness Rules, which were endorsed by the BPDG, were derived from the robustness provisions of numerous marketplace content protection agreements that were freely negotiated at arms' length between various parties. Examples include the 5C license agreement for DTCP, the Intel license agreement for HDCP, the 4C license agreement for CPRM, the PHILA and DFAST licenses, and the DVD CCA license agreement for CSS. It is thus fair to say that the Jointly Proposed Robustness Rules constitute a content protection industry "standard." This level and specificity of robustness has been determined in the marketplace to be optimal for the protection of copyrighted content over protected digital outputs and in protected recordings.[18] Given the goal of the Broadcast Flag regulation to bring digital

[18] It bears recalling that although recording of broadcast content is not prevented by the Broadcast Flag

broadcast content into the same protected realm as content distributed over other distribution channels such as cable, satellite, and DVDs, it only makes sense to model the Broadcast Flag robustness rules on those marketplace-derived rules used in other channels. Anything less would undermine the effectiveness of the regulation in achieving its goal.

The Jointly Proposed Robustness Rules represent a carefully crafted set of intertwined principles developed in marketplace negotiations by technical experts from various industries and numerous companies to deal with real-world experiences, threats, and limitations. They were not casually drafted nor put forward in this proceeding as a "wish list." The general standard found in Section X.7 of the Joint Proposal, that Covered Demodulator Products "shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such products to defeat the Demodulator Compliance Requirements," is found in numerous other content protection agreements. For instance, the 5C license agreement for DTCP provides that "Licensed Products . . . shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such Licensed Products to defeat the content protection requirements of DTCP . . . ."[19]

The Jointly Proposed Robustness Rules further specify the level of robustness in implementing the Compliance Rules and related rules governing content or sensitive aspects of product design: those rules are to be implemented in the product "in a reasonable method" such that they "[c]annot be defeated or circumvented" by using either general-purpose or specialized tools and equipment widely available at a reasonable price, and such that they "[*c*]*an only with difficulty be defeated or circumvented using professional tools or equipment . . . such as would*

regulation, protection of such recordings is essential to prevent unauthorized redistribution of the recorded content.

[19] 5C Adopter Agreement, Exh. C, ¶ 1.1; *see also, e.g.*, HDCP License Agreement, Exh. D, ¶ 1.1; DFAST ¶ 1.1; PHILA ¶ 1.1; CSS Procedural Specifications ¶¶ 6.2.4.1, 6.2.5.1.

be used primarily by persons of professional skill and training."[20] The second, italicized, component of this standard was critical to the Broadcast Flag solution, and it should be noted that in its initial comments in this proceeding, the IT Coalition did not propose any changes to that part of the provision.[21] For the reasons discussed above and further below, a standard which fails to impede professional or expert modifications which can then be easily proliferated and implemented by anyone undermines the effectiveness of the regulation in achieving its goal.

The practical, real-world experience of content owners and others suggests that such a level of robustness is necessary in order to prevent the widespread proliferation of hacks and unauthorized redistribution of content. As just one example, in 1999, a licensed software DVD player manufactured by Xing was released that contained only a minimal obfuscation of the device authorization keys. The Xing implementation thus violated the CSS robustness rules, which – like the Jointly Proposed Robustness Rules – required that secret data be encrypted or otherwise reasonably secured. However, the Xing player would have complied with the standard of robustness adopted by the Commission in this proceeding; ordinary users simply would not know where to look to find even a device authorization key left unprotected or minimally obfuscated.[22] Skilled hackers found the Xing authorization key and designed an executable software utility – DeCSS – that could be distributed worldwide via the Internet and would allow even novice users to download and use it to decrypt a DVD in their computers.[23] Fortunately,

[20] Joint Proposal § X.11; *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 3.5; HDCP License Agreement, Exh. D, ¶ 3.5; DFAST ¶ 3(e); PHILA ¶ 3(e); CPRM License ¶ 4.1; CSS Procedural Specifications ¶¶ 6.2.4.2, 6.2.5.2.

[21] See above, page 3 note 5.

[22] The MPAA is not conceding that, even under the Commission's robustness standard, DTV devices need not be manufactured so as to prevent the creation of "widely available tools" such as the DeCSS utility that could then be used to compromise other such devices. *See* page 20 below.

[23] *See Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 311-12 (S.D.N.Y. 2000).

because of the CSS robustness rules, the Xing player is an isolated case; indeed, it is the only such instance of a DVD device being successfully hacked of which the MPAA is aware. And, fortunately, the existence of the DMCA anti-circumvention provisions allowed content owners to pursue legal remedies against those distributing the DeCSS hacking utility. Such countermeasures would be infeasible, however, if every device could be legally manufactured to the inadequate level of robustness embodied in the Xing player.

The Xing case thus illustrates two lessons: first, as almost every privately negotiated content protection agreement and even the Commission itself has recognized, in order to protect content from unauthorized redistribution, it is not merely ordinary users that must be thwarted from hacking their devices, but experts such as those that hacked the Xing player and developed the DeCSS utility. Second, a high level of robustness such as that contained in the Jointly Proposed Robustness Rules will guide manufacturers in constructing devices that will better thwart most attacks. The point is thus not that compliant devices will never be hacked, nor that the regulation depends on all manufacturers always following the rules. Rather, it is simply the case that, as the marketplace for content protection has already demonstrated, the higher level of robustness contained in the Jointly Proposed Robustness Rules works. Reputable manufacturers will follow the rules, and those rules will thwart most attacks even by experts. Importantly, such a level of robustness will be equivalent to that being used for the construction of devices for other distribution channels. While content may never be absolutely secure, the adoption of the Jointly Proposed Robustness Rules in the Broadcast Flag regulation may make the difference between a content owner deciding whether it can or cannot trust the security of its content being delivered through the broadcast DTV channel.

The above examples represent what can happen when software implementation in a device is only insufficiently robust. Hardware implementation must be robust as well. For example, there must be no service menus discoverable by experts who can easily make them available to end users. Devices must be precluded from allowing the compliance rules to be defeated by, for instance, the press of a few buttons on a remote control that turns off the protection on an output. Such a situation is clearly in violation of the Jointly Proposed Robustness Rules,[24] but is only arguably a violation of the Commission's Robustness Rule. Once such an exploit is discovered by experts, the information could be quickly disseminated via Internet chat rooms and web pages to novice users. If all DTV devices are designed in such a manner, the inevitable result would be a widespread defeat of broadcast DTV content protection.

Other industries have similarly learned from experience why a high standard of robustness is necessary to prevent the widespread distribution of hacks or hacked content. Cable programmers and satellite broadcasters have for years fought a battle against professional thieves that break the protection schemes of their satellite signals and sell modified equipment or smartcards to ordinary users to receive unauthorized service. For example, in the late 1980s, hackers were able to modify receiving devices for satellite signals based on the VideoCipher encryption scheme, and began selling modified equipment in such quantities that it is estimated that as much as half of all satellite boxes were unauthorized.[25] Since then, cable and satellite companies have deployed increasingly robust products, and have dramatically decreased the rate of piracy. While hacked smartcards are still a widespread problem, both industries are profitable. Video game console and cell phone manufacturers have also learned to make their products more robust, again successfully limiting hacks to the point where they do not threaten

[24] *See* Joint Proposal § X.7(b)(3).

[25] *See* Charles Platt, *Satellite Pirates*, Wired, Aug. 1994 (describing hackers in Bahamas using EPROMs and heat guns to hack VideoCipher boards).

the viability of those industries.[26] It is the robustness of DVD devices, cable and satellite receivers, video game consoles, and cell phones that makes the difference between the situation of those industries and the situation of the music industry, where all content is in the clear and is instantly made available worldwide on peer-to-peer networks.

A high level of robustness is therefore necessary in order to raise the level of difficulty necessary to gain unauthorized access to content in the clear. The robustness rules in the Broadcast Flag regulation must also be explicit in order to adequately ensure that device manufacturers have the guidance required to build robust products.[27] That is why the Jointly Proposed Robustness Rules, like the marketplace-derived agreements on which they were based, also listed the specific steps that must, at a minimum, be taken to make products robust. For example, a number of practices known to be insecure must be specifically prohibited. Thus, the Jointly Proposed Robustness Rules prohibited Covered Demodulator Products from including certain hardware elements that readily permit Compliance Rules to be defeated, or from being constructed so as to enable discovery of secret keys or algorithms that underlie implementation of compliant technologies.[28] The Joint Proposal and the marketplace content protection agreements on which it was based also prohibit allowing unencrypted, compressed data to be present on any User Accessible Bus, such as PCMCIA, Cardbus, or PCI buses.[29] Unencrypted,

[26] *See* Seth Schiesel, *Some Xbox Enthusiasts Microsoft Didn't Aim For*, N.Y. Times, July 10, 2003, at G1; Mike Dano, *Nokia to Add Security Features to Games After N-Gage Is Hacked*, RCR Wireless News, Nov. 17, 2003, at 6.

[27] It is worth noting that the IT industry had no objections in the BPDG to any of the Jointly Proposed Robustness Rules, including not only the higher level of robustness but also the specific steps to make products more robust discussed here. *See* Joint Proposal at 1 (noting that proposal is on behalf of, in part, the Computer Industry Group).

[28] *See* Joint Proposal § X.7(b), (c); *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶¶ 1.2, 1.3; HDCP License Agreement, Exh. D, ¶¶ 1.1, 1.2; DFAST ¶¶ 1.2, 1.3; PHILA ¶¶ 1.2, 1.3; CPRM License ¶¶ 1.2 – 1.4; CSS Procedural Specifications ¶ 6.2.5.2(b)(iii).

[29] *See* Joint Proposal § X.8; *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 2; HDCP License Agreement,

compressed data is particularly susceptible to being intercepted and siphoned if found on a User Accessible Bus due to its diminished data rate, which allows content to be easily captured and redistributed.[30]

The Joint Proposal, following in the footsteps of marketplace-derived agreements, further specified that products follow certain techniques known to make products more robust. The Jointly Proposed Robustness Rules required that, when compressed Marked or Unscreened Content is flowing between portions of the Covered Demodulator Product, those portions must remain integrated and the content remain "reasonably secure from being intercepted or copied except as permitted under the Demodulator Compliance Requirements."[31] Those portions of the product that are implemented in software must secure secret keys or algorithms by a "reasonable method" such as encryption or other recognized techniques, and must be designed with self-checking mechanisms such that unauthorized modifications will cause a failure to provide access to the content.[32] Those portions of the product that are implemented in hardware must also secure secret keys or algorithms by a "reasonable method" for hardware, such as embedding, and be designed so that attempts to modify the hardware "would pose a serious risk" of rendering the Covered Demodulator Product unable to use digital broadcast content.[33] Interfaces between

Exh. D, ¶ 2; DFAST ¶ 2; PHILA ¶ 2; CPRM License ¶ 2; CSS Procedural Specifications ¶¶ 6.2.4.2(2), 6.2.5.2(b)(ii).

[30] The Joint Proposal, like the 5C license and the CSS Procedural Specifications, contained a provision that would allow the Robustness Rules to be altered in the event that uncompressed content poses too great a risk when found on a User Accessible Bus. *See* Joint Proposal § X.8(a); 5C Adopter Agreement, Exh. C, ¶ 2.2; CSS Procedural Specifications ¶¶ 6.2.4.2(2), 6.2.5.2(b)(iv).

[31] Joint Proposal § X.9(a); *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 3.1; HDCP License Agreement, Exh. D, ¶ 3.1; DFAST ¶ 3(a); PHILA ¶ 3(a); CSS Procedural Specifications ¶ 6.2.4.2(2).

[32] Joint Proposal § X.9(b); *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 3.2; HDCP License Agreement, Exh. D, ¶ 3.2; DFAST ¶ 3(b); PHILA ¶ 3(b); CPRM License ¶ 3.1; CSS Procedural Specifications ¶ 6.2.4.1.

[33] Joint Proposal § X.9(c); *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 3.3; HDCP License Agreement, Exh. D, ¶ 3.3; DFAST ¶ 3(c); PHILA ¶ 3(c); CPRM License ¶ 3.2; CSS Procedural Specifications ¶ 6.2.5.1.

hardware and software components must also be secure.[34]

The Jointly Proposed Robustness Rules also allowed device manufacturers to use entirely self-certified output protection technologies (i.e., those that need not be identified as an Authorized Digital Output Protection Technology) in certain limited circumstances. In these limited circumstances, the Jointly Proposed Robustness Rules allow content to be output protected by a "Robust Method," meaning, in the case of add-in computer products (e.g., a DTV tuner card), a method that makes content "reasonably secure from being intercepted, redistributed, or copied when being so passed," and in the case of outputs of Unscreened, pre-processed content to a Peripheral TSP Product, a method that is "at least as effective" as an Authorized Digital Output Protection Technology.[35] This provision is unique to the Broadcast Flag regulation, and was inserted at the request of the IT industry; most other content protection schemes require all digital outputs to be approved under the license. Both accommodations were made to allow IT manufacturers full flexibility in designing their devices.[36] The adoption of an effective robustness provision, however, was essential to the compromise that permitted use of self-certified technologies in these limited circumstances.

Drawing on previous marketplace agreements, the Joint Proposal additionally specified a very important mechanism for robustness standards to evolve in light of new developments, a mechanism also used in marketplace agreements.[37] Section X.12 of the Joint Proposal provided

[34] Joint Proposal § X.9(d); *see also, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 3.4; HDCP License Agreement, Exh. D, ¶ 3.4; DFAST ¶ 3(d); PHILA ¶ 3(d); CPRM License ¶ 3.3.

[35] Joint Proposal § X.10.

[36] With respect to outputs pursuant to Section 73.9003(a)(4), content that has not undergone Transport Stream Processing poses less of a risk of interception and redistribution than content that has been processed, and therefore a limited exception to the Compliance Rules was made in order to permit IT products that demodulate a signal but convey the signal to another product for processing. With respect to Section X.6(a), the exception was made to account for IT practices in designing "open architecture" products.

[37] *See, e.g.*, 5C Adopter Agreement, Exh. C, ¶ 3.7; HDCP License Agreement, Exh. D, ¶ 3.6; DFAST ¶ 3(f);

that, in the event that circumstances changed such that products that were robust when manufactured no longer satisfied that standard, then the manufacturer would have to cease distribution of the non-robust product within eighteen months, and thereafter distribute only products that were robust in light of the changed circumstances. This provision gives a manufacturer ample time to change its product design in the event of a compromise. It is true that the Commission's existing Robustness Rule may require manufacturers to re-design products if a utility such as DeCSS that can be used by ordinary users becomes "widely available at a reasonable price." Nevertheless, this aspect of the Commission's Robustness Rule does not capture the obligation to design products to account for new circumstances that may not be readily classified as a "tool" capable of being wielded by ordinary users. Without specifying a provision such as Section X.12, the Commission's Robustness Rule may eventually come to embody a superseded set of norms that no longer reasonably ensures the security of devices from attack.

C. **Device Manufacturers Would Suffer No Harm from a Higher Level of Robustness**

Device manufacturers have demonstrated repeatedly that no intolerable burden is imposed on them by the Robustness Rules contained in the Joint Proposal. Nearly identical robustness rules have been negotiated and adopted by manufacturers in numerous other agreements, such at the 5C license for DTCP, the 4C license for CPRM, the Intel license for HDCP, the DFAST and PHILA licenses for cable devices, and the DVD CCA license for CSS. As those adopters have recognized, the Jointly Proposed Robustness Rules allow IT and CE manufacturers a wide range of "flexibility in determining how to effectuate [the] compliance

PHILA ¶ 3(f); CPRM License ¶ 5; CSS Procedural Specifications ¶¶ 6.2.4.3, 6.2.5.5.

rules and to ensure the security of content."[38] That is why barely any objection was raised to the Robustness Rules in the BPDG. The Robustness Rules in the Joint Proposal are thus a market standard, departure from which is unwarranted given the premise of the Broadcast Flag regulation to give broadcast television protection equivalent to other distribution channels.

Furthermore, the burden will be minimal on manufacturers of digital CableCard-compatible receivers with integrated DTV broadcast tuners implementing the Jointly Proposed Robustness Rules, given the similarity of the robustness rules of the PHILA and DFAST licenses. All such products will need to adhere to a level of robustness compatible with obligations imposed on them under the cable or satellite content protection schemes, which include the detailed Jointly Proposed Robustness Rules. Inclusion of the same Robustness Rules for handling broadcast content in such devices would thus represent no additional burden.

To the extent that the IT Coalition suggests that DTV broadcast content deserves a lower standard of robustness because it is "delivered over-the-air in the clear," that observation misses the entire point of the regulation.[39] The purpose of the Broadcast Flag regulation is to "ensure the continued availability of high value DTV content to consumers through broadcast outlets," which will only occur if broadcast DTV is equally secure as other potential digital distribution channels that can use encryption at the source. The regulation achieves this by requiring devices to behave *as if* broadcast television content was received in a protected form, and to ensure that protection going forward from the point of reception. It is simply misguided to suggest that, because broadcast DTV is not already encrypted, it should not receive the level of protection as provided by the very distribution channels with which DTV broadcasters will be in competition.

[38] Broadcast Flag Order ¶ 46. The Commission's concern is therefore already addressed in the Jointly Proposed Robustness Rules.

[39] *See* Comments of the IT Coalition (filed Dec. 6, 2002) at 27 n.64.

There are, unfortunately, manufacturers who oppose all content protection regulations and will take any opportunity to undermine them. The weaker robustness standard adopted in the Commission's Robustness Rule offers such companies the opportunity to do just that with respect to the Broadcast Flag regulation. Such companies will be able to build DTV products that contain only the bare minimum of robustness required – that is, they will at most thwart only the "ordinary user using generally-available tools or equipment." Although compliant with the regulation, such devices will be widely hacked, the hacks will be widely disseminated to ordinary users, and the result may be rampant redistribution of DTV content.

D. <u>Other Mechanisms Short of Restoring the Market-Defined Jointly Proposed Robustness Rules Cannot Address The Problem</u>

The Broadcast Flag Regulation must incorporate the market-derived Jointly Proposed Robustness Rules. Other means of attempting to resolve the issue will have no effect. For example, if it is suggested that the revocation procedures for Authorized Digital Output Protection Technologies and Recording Methods be used to address compromises, that will not solve the problem. Revoking a Authorized Digital Output Protection Technology or Recording Method will have no impact whatsoever on the robustness of the Flag detection in an individual device. Since Authorized Digital Output Protection Technologies and Recording Methods are triggered downstream, their revocation will have no impact on the security of the upstream content.

Nor is the Commission's request that "manufacturers consult with content owners on how to best achieve DTV content security" likely to produce a solution to the level of robustness required by this regulation.[40] Although the Commission is correct that the "'ordinary user' level

[40] Broadcast Flag Order ¶ 46.

of robustness represents a floor that manufacturers are free to exceed," manufacturers will have no incentive to exceed the floor. The very reason the Broadcast Flag is needed is because content owners have no privity with device manufacturers when it comes to broadcast content. Since broadcast television is provided over-the-air for free, there is nothing the content owner can selectively grant or withhold from the device manufacturer to encourage the manufacturer to reach an agreement with the content owner. Discussions of robustness are therefore likely to be unproductive.

Nor is there much comfort in the fact that even under the Commission's Robustness Rule, device manufacturers would have to protect against a software hack created by one individual and then freely distributed as "generally available tool." Even in such a circumstance, once the hack became generally available, the harm would already have been wreaked for that class of devices, which would persist as a noncompliant legacy into the future. That is why the robustness standard must be high enough to prevent most such hacks from occurring in the first place.

E. The Jointly Proposed Robustness Rules Should Be Made Effective Eighteen Months After They Are Adopted

Of primary importance is that nothing be allowed to delay implementation of the Broadcast Flag regulation. There is no reason why adoption of the revised Robustness Rules should delay implementation of the existing regulation as an interim measure in July 2005. The MPAA proposes that the Commission should grant device manufacturers eighteen months from the time of public notice of the adoption of the Jointly Proposed Robustness Rules to implement the revised robustness standard. As provided in Section 73.9002 of the existing regulation, all Covered Demodulator Products sold or distributed subsequent to that time would be required to be compliant with the revised regulation.[41]

II. **The Commission Should Clarify the Obligation of Manufacturers of Add-in Computer Products Using Robust Method Transfers to Ensure that Marked and Unscreened Content Is Not Available in Unencrypted, Compressed Form Via a User Accessible Bus**

The Commission adopted Section X.6 of the Joint Proposal nearly verbatim, with one important difference. Section X.6 as set forth in the Joint Proposal provided:

> Where a Covered Demodulator Product passes Unscreened Content or Marked Content from such Covered Demodulator Product to another product, other than where such Covered Demodulator Product passes, or directs to be passed, such content to an output . . . , it shall so pass such content (a) using a Robust Method; or (b) protected by an Authorized Digital Output Protection Technology . . . , in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology. Neither Unscreened Content nor Marked Content may be so passed in unencrypted, compressed form via a User Accessible Bus.

Thus, the last sentence, banning the use of unencrypted, compressed content, applied to both Robust Method transfers and outputs over Authorized Digital Output Protection Technologies. This is important because unencrypted, compressed content is susceptible to being intercepted and should never be present where it can be easily accessed.

The Commission, however, when reformatting this item for better readability, omitted an important paragraph break before the last sentence. Section 73.9006 now reads:

> (a) Where a covered demodulator product passes unscreened content or marked content to another product, other than where such covered demodulator product passes, or directs such content to be passed to an output . . . , it shall pass such content:
>
> (1) Using a robust method; or
>
> (2) Protected by an authorized digital output protection technology . . . in accordance with any applicable obligations established as a part of its approval pursuant to

[41] *See* 47 C.F.R. § 73.9002.

> Sec. 73.9008. *Neither unscreened content nor marked content may be so passed in unencrypted, compressed form via a User Accessible Bus.*

(Emphasis added.) The inclusion of the last, italicized sentence with Paragraph (2), rather than standing alone so that it clearly modifies both Paragraphs (1) and (2), makes it potentially ambiguous whether the obligation of that sentence applies to merely Authorized Digital Output Protection Technologies or to Robust Methods as well. The Commission should clarify that no outputs for computer add-in products should be allowed to expose unencrypted, compressed data over a User Accessible Bus, whether protected by an Authorized Digital Output Protection Technology or by a Robust Method.

<u>CONCLUSION</u>

In adopting the Broadcast Flag regulation, the Commission has done a commendable job in establishing an important baseline for broadcast DTV protection. However, the Commission should complete its work by adopting specific, robustness standards derived from existing marketplace practices that appropriately support the Commission's Compliance Rules. The revisions suggested here will help the Commission to achieve its goal of "ensur[ing] the continued availability of high value DTV content to consumers through broadcast outlets." Broadcast Flag Order ¶ 8. We therefore respectfully request that the Commission reconsider its decision and adopt the Jointly Proposed Robustness Rules attached hereto at Exhibit A; and clarify Section 73. 9006(a) as set forth above.

Respectfully submitted,

MOTION PICTURE ASSOCIATION OF AMERICA, INC.

By: Bruce E. Boyden

Jon A. Baumgarten
Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street NW, Suite 800
Washington, DC 20036
(202) 416-6800

Counsel for The Motion Picture Association of America, Inc.